Technical Cybersecurity

Phishing

Phishing always works.

PENTESTS USUALLY DON’T ALLOW IT

- It doesn’t mean much
- Somebody always falls for it

VARIETY OF PAYLOADS

- MS Office documents (Word, Excel)
- Many folks will run macros on a document from their boss

Spearphishing

Phishing on steroids

- Emails are targeted
- Messages are well crafted and written
- Sender is well known to recipient
- Sent at times to minimize follow up

Phishing will target an entire organization

- …spearphishing just targets a few members

Information

WHO'S THE TARGET

- You need to find someone in the organization

WHO DOES THE TARGET KNOW

- Who does the target work for and with? often this is on the company website or in a directory

WHAT IS THE CONTEXT

- What kinds of things are going on between the target and the forged sender?

WHEN WOULD THAT EMAIL BE SENT

- When is the target not likely to follow up? when the sender is on vacation? on a trip in another time zone?

Case: BlackEnergy 2 & 3

BlackEnergy campaigns reliant on phishing

- Powerpoint
- Excel
- Word

Spearphished recipients

- Used various messages to get them to open attachments
- Users agreed to run macros
- Macros downloaded and installed small dropper
- Dropper then downloads and installs other payloads

BlackEnergy didn’t use a single exploit.